

FAEGRE DRINKER BIDDLE & REATH LLP

Matthew J. Fedor
600 Campus Drive
Florham Park, New Jersey 07932
(973) 549-7000
(973) 360-9831 (fax)
Matthew.Fedor@faegredrinker.com

Zoë K. Wilhelm
1800 Century Park East, Suite 1500
Los Angeles, California 90067
(310) 203-4000
(310) 229-1285 (fax)
Zoe.Wilhelm@faegredrinker.com

*Attorneys for Defendant
Quest Diagnostics Incorporated*

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

ANGELA COLE and BEATRICE
ROCHE, individually and on behalf
of all others similarly situated,

Plaintiffs,

v.

QUEST DIAGNOSTICS, INC.,

Defendant.

Case No. 2:23-cv-20647-WJM-JSA

Civil Action

(Document Filed Electronically)

Motion Day: March 4, 2024

ORAL ARGUMENT REQUESTED

**DEFENDANT'S BRIEF IN SUPPORT OF ITS
MOTION TO DISMISS PLAINTIFFS'
FIRST AMENDED CLASS ACTION COMPLAINT**

TABLE OF CONTENTS

INTRODUCTION	1
STATEMENT OF FACTS	4
A. The Parties	4
B. MyQuest Account Terms & Conditions	4
C. Quest’s Cookie Notice and Privacy Notice.....	6
1. All Quest website visitors agree to Cookie and Privacy Notices.	6
2. MyQuest Users Separately Agree to Privacy and Cookie Notices.	9
D. Website Access and the Facebook Pixel.....	11
E. Plaintiffs’ Experience on Quest’s Websites.....	12
F. Plaintiffs’ Facebook Status.....	14
G. Plaintiffs’ Claims.....	16
STANDARD OF REVIEW	17
ARGUMENT	19
I. Plaintiffs’ Claims Fail Because They Did Not Plausibly Allege Lack of Consent to the Data Collection Practices at Issue.	19
II. Plaintiffs’ CIPA Claim Fails Because Under Third Circuit Law Facebook Was A Party to the Communications At Issue.	24
III. Plaintiffs’ CIPA Claim Fails Because They Did Not Plausibly Allege that the “Contents” of Their Communications Were Intercepted.	27
IV. Plaintiffs’ CMIA Claim Fails Because None of the Information Allegedly Disclosed or Used Constitutes “Medical Information.”	31
V. Plaintiffs’ CMIA Claim Fails Because They Do Not Allege that Quest Was the Party that Disclosed or Used the Information At Issue.....	35
VI. Plaintiffs’ California Claims Fail Because New Jersey Law Applies.....	37
CONCLUSION	40

TABLE OF AUTHORITIES

Cases	Page(s)
<i>In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.</i> , 2023 WL 8540911 (D.N.J. May 5, 2023).....	32
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	18
<i>Bailey v. CVS Pharmacy, Inc.</i> , 2018 WL 3866701 (D.N.J. Aug. 14, 2018)	20
<i>Bambi Baby.com Corp. v. Madonna Ventures, Inc.</i> , 2019 WL 2337447 (D.N.J. June 3, 2019).....	19
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	17, 18
<i>Blue Sky 1, LLC v. Jaguar Land Rover N. Am., LLC</i> , 2016 WL 6803081 (D.N.J. Nov. 16, 2016)	19
<i>Brodsky v. Apple, Inc.</i> , 445 F. Supp. 3d 110 (N.D. Cal. 2020).....	27
<i>Bycko v. State Farm Mut. Auto. Ins. Co.</i> , 2023 WL 7411752 (D.N.J. Nov. 9, 2023)	34
<i>Coface Collections N. Am. Inc. v. Newton</i> , 430 F. App'x 162 (3d Cir. 2011)	39
<i>Cole v. Quest Diagnostics, Inc.</i> , 2023 WL 6201702 (E.D. Cal. Sept. 22, 2023)	<i>passim</i>
<i>Collins v. Mary Kay, Inc.</i> , 874 F.3d 176 (3d Cir. 2017)	37, 38
<i>Diversant, LLC v. Carino</i> , 2018 WL 1610957 (D.N.J. Apr. 2, 2018).....	38, 39
<i>Eichenberger v. ESPN, Inc.</i> , 2015 WL 7252985 (W.D. Wash. May 7, 2015)	35

<i>Eisenhower Medical Center v. Superior Court</i> , 226 Cal. App. 4th 430 (Cal. Ct. App., 4th Dist. 2014)	31, 32, 33
<i>Garcia v. Enter. Holdings, Inc.</i> , 78 F. Supp. 3d 1125 (N.D. Cal. 2015)	20, 22
<i>In re Google Assistant Privacy Litig.</i> , 457 F. Supp. 3d 797 (N.D. Cal. 2020)	20
<i>In re Google Inc. Cookie Placement Consumer Priv. Litig.</i> , 806 F.3d 125 (3d Cir. 2015)	<i>passim</i>
<i>Hammerling v. Google LLC</i> , 615 F. Supp. 3d 1069 (N.D. Cal. 2022)	28, 29
<i>Heller v. Norcal Mut. Ins. Co.</i> , 8 Cal. 4th 30 (1994)	20
<i>Homa v. Am. Express Co.</i> , 558 F.3d 225 (3d Cir. 2009), <i>abrogated on other grounds by AT&T</i> <i>Mobility LLC v. Concepcion</i> , 563 U.S. 333 (2011)	38
<i>In re Hulu Privacy Litig.</i> , 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014)	35
<i>Kurowski v. Rush Sys. for Health</i> , -- F. Supp. 3d --, 2023 WL 4707184 (N.D. Ill. July 24, 2023)	32
<i>Mayer v. Belichick</i> , 605 F.3d 223 (3rd Cir. 2010)	18
<i>Medimatch, Inc. v. Lucent Techs. Inc.</i> , 120 F. Supp. 2d 842 (N.D. Cal. 2000)	40
<i>In re Nickelodeon Consumer Privacy Litig.</i> , 2014 WL 3012873 (D.N.J. July 2, 2014), <i>aff'd</i> 827 F.3d 262 (3d Cir. 2016)	27, 28, 29, 35
<i>Oliver v. Noom, Inc.</i> , 2023 WL 8600576 (W.D. Pa. Aug. 22, 2023)	23
<i>Perkins v. LinkedIn Corp.</i> , 53 F. Supp. 3d 1190 (N.D. Cal. 2014)	20, 23

<i>Phillips v. Cnty. of Allegheny</i> , 515 F.3d 224 (3rd Cir. 2008)	18
<i>Popa v. Harriet Carter Gifts, Inc.</i> , 426 F. Supp. 3d 108 (W.D. Pa. 2019).....	23
<i>Rajan v. Crawford</i> , 2022 WL 16646690 (3rd Cir. Nov. 3, 2022)	18
<i>Regents of Univ. of Cal. v. Superior Court</i> , 220 Cal. App. 4th 549 (Cal. Ct. App., 2d Dist. 2013)	36
<i>Silver v. Stripe Inc.</i> , 2021 WL 3191752 (N.D. Cal. July 28, 2021)	22
<i>Smith v. Facebook, Inc.</i> , 262 F. Supp. 3d 943 (N.D. Cal. 2017), <i>aff'd</i> 745 F. Appx. 8 (9th Cir. 2018)	<i>passim</i>
<i>Smith v. Trusted Universal Standards in Elec. Transactions, Inc.</i> , 2010 WL 1799456 (D.N.J. May 4, 2010).....	30
<i>Stasi v. Inmediata Health Grp. Corp.</i> , 501 F. Supp. 3d 898 (S.D. Cal. 2020).....	36
<i>Wilson v. Rater8, LLC</i> , 2021 WL 4865930 (S.D. Cal. Oct. 18, 2021)	32, 33
<i>Yoon v. Lululemon USA, Inc.</i> , 549 F. Supp. 3d 1073 (C.D. Cal. 2021)	29, 30
<i>In re Zynga Privacy Litig.</i> , 750 F.3d 1098 (9th Cir. 2014)	27, 28, 29
Statutes, Rules & Regulations	
Cal. Civ. Code § 56.05(j)	31
Cal. Civ. Code § 56.10(a)	<i>passim</i>
Cal. Civ. Code § 56.10(d)	1, 20, 36
Cal. Pen. Code § 631	<i>passim</i>

Cal Pen. Code § 631(a)19, 27

N.J.S.A. 2A:156A-339

Other Authorities

Restatement (Second) Conflicts § 187(2).....38, 39

INTRODUCTION

This case is part of a wave of recent privacy litigation against website owners regarding the “Facebook Pixel,” a common website analytics tool that uses “cookies” to collect data regarding user activity on websites to understand and measure interest in products and services, and to better serve users. Plaintiffs assert that the use of the Pixel on websites owned by Quest Diagnostics Incorporated¹ enabled Facebook² to collect data regarding Plaintiffs’ use of Quest’s websites. Their theory is that Facebook “intercepted” and “eavesdropped” on their internet communications with Quest in violation of the California Invasion of Privacy Act, Cal. Pen. Code § 631 (“CIPA”).

Even though (1) Quest discloses the data collection practices that Plaintiffs challenge, and (2) the alleged eavesdropper is *Facebook*, Plaintiffs assert a unique theory of CIPA liability *against Quest*. Specifically, Plaintiffs claim that Quest “aid[ed] and assist[ed] Facebook’s eavesdropping” simply by using the Pixel. Plaintiffs also allege improper disclosure or use of unspecified “medical information” in violation of the California Confidentiality of Medical Information Act (“CMIA”), Cal. Civ. Code § 56.10(a), (d). Plaintiffs seek statutory damages under CIPA and CMIA on behalf of a California class of Quest website users.

¹ Quest was erroneously named as “Quest Diagnostics, Inc.”

² For ease of reference and to remain consistent with Plaintiffs’ use of defined terms, Quest refers to Meta Platforms, Inc. by its former name, Facebook.

While this case was pending in the Eastern District of California, Plaintiffs filed a First Amended Complaint (“FAC”) in response to Quest’s motion to dismiss. The two minor changes they made did not fix the fundamental defects in their claims, and Quest moved to dismiss the FAC. Since the filing of that motion in February 2023, Plaintiffs’ already weak claims have gotten materially worse.

On September 22, 2023, E.D. Cal. District Judge Jennifer Thurston granted Quest’s motion to transfer venue to this Court in accordance with the forum selection clause in the “Quest Diagnostics Patient Registration: Terms and Conditions” (“Account Terms & Conditions”). In so doing, Judge Thurston made two key findings that further doom Plaintiffs’ claims: (1) that Plaintiffs agreed to the Account Terms & Conditions; and (2) “the Terms and Conditions disclose the data collection practices challenged and referenced by Plaintiffs.” *Cole v. Quest Diagnostics, Inc.*, 2023 WL 6201702, at *3-4 (E.D. Cal. Sept. 22, 2023). In accordance with Your Honor’s instruction to update the motion papers in light of the transfer to this Court, Quest renews its motion to dismiss the FAC. As explained in further detail below, Plaintiffs did not—and cannot—assert viable claims under CIPA or CMIA.

First, lack of consent/authorization is a necessary element of their CIPA and CMIA claims. But Plaintiffs did not—and cannot—plausibly allege that they did not consent to the data collection practices at issue. Indeed, Judge Thurston already

found that the Account Terms and Conditions that Plaintiffs agreed to “disclose the data collection practices challenged and referenced by Plaintiffs.” Plaintiffs also agreed to the data collection practices at issue by agreeing to Facebook’s policies.

Second, under Third Circuit law, Facebook is the intended recipient of—and a party to—the communications at issue. As a matter of law, Facebook cannot “intercept” or “eavesdrop” on communications to which it is a party. It necessarily follows that Quest could not have violated CIPA for purportedly “aiding and assisting Facebook’s” receipt of the communications at issue.

Third, Plaintiffs’ CIPA claim fails because they have failed to plausibly allege that the use of the Pixel caused the “contents” of their internet communications to be intercepted within the meaning of CIPA.

Fourth, Plaintiffs’ CMIA claim fails because none of the information at issue constitutes “medical information” as defined by the statute.

Fifth, Plaintiffs’ CMIA claim fails because Plaintiffs failed to plausibly allege that Quest affirmatively disclosed or used the information at issue. Indeed, their theory is that *Facebook* “intercepted” the communications.

Finally, the only claims Plaintiffs assert arise under California law, which does not apply. Indeed, the Account Terms & Conditions contain a choice of law clause requiring application of New Jersey law. As a result, Plaintiffs’ California statutory claims fail as a matter of law.

STATEMENT OF FACTS³

A. The Parties

Quest is headquartered in New Jersey and is a leading provider of diagnostic services, providing clinical laboratory testing to millions of customers. FAC ¶ 2.

Among the websites Quest operates are www.questdiagnostics.com (the “General Website”), which is accessible to the public, and myquest.questdiagnostics.com (“MyQuest”), which requires users to login via an account. *Id.* ¶ 1.⁴

Plaintiffs Angela Cole and Beatrice Roche reside in California. Cole alleges that she created a MyQuest account in or around August 2019, and Roche alleges that she created a MyQuest account in or around March 2022.⁵ *Id.* ¶¶ 4-5.

B. MyQuest Account Terms & Conditions

To create MyQuest accounts on the MyQuest website, users must go through a multi-step process and enter various information (name, address, email, etc.).

Declaration of Michael Rigal (“Rigal Decl.”) ¶ 4.⁶ At the final step of the process,

³ For purposes of this motion only, Quest assumes the truth of all well-pleaded allegations in the FAC.

⁴ The FAC refers to MyQuest as the “Patient Protected Website.” FAC ¶ 1.

⁵ In the original Complaint filed on July 19, 2022, Roche alleged that she created a MyQuest account “[a]pproximately four months ago,” which translates to March 2022. *See* Declaration of W. Joshua Lattimore (“Lattimore Decl.”), Ex. A ¶ 5. In what was likely an oversight, Roche repeated the same “[a]pproximately four months ago” allegation in the FAC filed on January 6, 2023. FAC ¶ 5. Quest assumes the truth of the allegation in the original Complaint regarding the timing of Roche’s MyQuest account creation.

⁶ Plaintiffs allege they signed up for MyQuest accounts and their access to those accounts and use of Quest’s websites is integral to their allegations. FAC ¶¶ 4-5.

users must click a green button at the bottom of the screen that reads, “Create Account.” *Id.* ¶ 6 & Ex. A. The last text on the screen before the “Create Account” button is a section with the heading “Terms & Conditions” written in bold text, where users are informed that “By clicking ‘Create account’, I accept the Terms and Conditions.” *Id.* The words “Terms and Conditions” are a hyperlink in green font, which is different than the color of the surrounding text. *Id.*

Clicking on the Terms and Conditions hyperlink opens the full text of the Account Terms & Conditions. *Id.* ¶ 7. If the user does not click the “Create Account” button and accept the Account Terms & Conditions, a MyQuest account is not created. *Id.* ¶ 8.

The opening paragraph of the Account Terms & Conditions states: “By accessing or using the Account Service, you agree to be bound by these terms and conditions (this ‘Agreement’).” *Id.*, Ex. B. The paragraph entitled “Scope of Service” states, “[t]his Agreement applies to your use of the Account Service,” which “provides a variety of content, products and services, including diagnostic health testing and services, data analysis, . . . and the ability to connect with third

They also quote certain aspects of the General Website (namely, Quest’s Cookie Notice) in the FAC. *Id.* ¶ 41, figs. 12 & 13. Thus, the Account Terms & Conditions, the Cookie Notice, the related Privacy Notice, and other aspects of the websites are all incorporated by reference, and the Court may consider them at this stage. *See infra* at pp. 18-19. In the alternative, all of these items are publicly available and thus are properly subject to judicial notice as their existence and accuracy cannot reasonably be questioned.

parties.” *Id.* Finally, Paragraph 12, entitled “Applicable Law,” provides that “any and all disputes related to this Agreement shall be construed in accordance with the laws of the State of New Jersey” and “You agree that the statutes and laws of the State of New Jersey, without regard to any principles of conflicts of law, will apply to any and all matters relating to the use of the Account Service.”⁷ *Id.*

C. Quest’s Cookie Notice and Privacy Notice

1. All Quest website visitors agree to Cookie and Privacy Notices.

All visitors to Quest’s website are subject to Quest’s Cookie Notice and Privacy Notice.⁸ At the time Plaintiffs commenced this litigation, a pop-up banner on the General Website read:

We and our partners use cookies to enhance user experience, analyze performance and traffic on our website, and personalize content. We also share information about your use of our website with our advertising and analytics partners. For more information on our use of

⁷ The Terms and Conditions applicable to use of the General Website contain a similar choice of law clause, which states, “you agree that the statutes and laws of the State of New Jersey, without regard to any principles of conflicts of law, will apply to all matters relating to the use of this site.” Declaration of Keena Hausmann (“Hausmann Decl.”) ¶¶ 14-15, Ex. H § 12.

⁸ Over time, Quest has had different iterations of the Cookie Notice and Privacy Notice, and the policies have had slightly different names. Hausmann Decl. ¶ 6. In 2019, for example, Quest had an “Online Privacy Policy” and a “Website Cookies Notice and Disclosure Statement.” *Id.* Plaintiff Roche allegedly visited Quest’s websites in March 2022 and Plaintiff Cole allegedly visited Quest’s websites in August 2019. FAC ¶¶ 4-5. For ease of reference, this brief focuses on the policies and processes in effect at the time the original Complaint was filed because Plaintiffs reference them in the FAC, *see, e.g.*, FAC ¶ 41, figs. 12 & 13, make no attempt to distinguish between the various policies over different points in time, and have not plausibly alleged lack of consent (as discussed *infra*).

cookies and information about your use of our site, please see our **Cookie Policy** and **Privacy Policy**. You can also manage your cookie choices by visiting Cookie Settings.

Hausmann Decl. ¶ 10, Ex. E (italicized emphasis added). “Cookie Policy” and “Privacy Policy” were in bold text and were hyperlinks that, when clicked, took users to the applicable Cookie Notice and Privacy Notice, respectively. *Id.* ¶ 11. At the time Plaintiffs commenced this litigation, visitors could click “Accept Cookies” or “Cookie Settings,” the latter of which took the visitor to the “Privacy Preference Center,” which further explained:

When you visit our website, we store cookies on your browser to collect information about you, your preferences, or your device in order to make the site work as you expect it to and to provide a more personalized web experience. You can choose not to allow certain types of cookies, but that may impact your experience of our website and the services we are able to offer. Click on the different category headings to find out more about the different kinds of cookies we use.

Id. ¶ 12, Ex. F (emphases added). The Privacy Preference Center allowed visitors to not allow use of certain cookies. *Id.* If a website visitor did not interact with the pop-up banner on the homepage, it continued to appear on other pages. *Id.* ¶ 12.

Quest’s Cookie Notice further explains that Quest uses “cookies to track responses and views of our advertisements,” as well as “pixels.”⁹ *Id.*, Ex. D. The Cookie Notice describes specific types of cookies Quest uses and what information

⁹ The version of the Cookie Notice in effect at the time Plaintiffs filed the original Complaint had been in effect since December 17, 2020. Hausmann Decl. ¶ 9.

each will collect. *Id.* Plaintiffs quote portions of Quest’s Cookie Notice in the FAC that detail Quest’s use of “Performance Cookies” and “Targeting Cookies.” FAC ¶ 41, figs. 12 & 13.

Performance Cookies “collect information about how visitors use a website [but] do not collect information that identifies a specific visitor.” FAC ¶ 41, fig. 13. The information Quest “gather[s] through performance cookies is used to improve how the websites work, to help us evaluate website usage, **makes our marketing more relevant**, and improves your experience.” *Id.* (emphasis added).

Targeting Cookies “**are used to deliver online advertisements both on and off websites visited that may be more relevant to visitor interests based on activity from a website being browsed and based on a profile built of visitor interests.**” FAC ¶ 41, fig. 12 (emphasis added). Quest informs website visitors that “**We use targeting cookies . . . on our sites to help us promote Quest’s products and services to you on *other* sites and platforms. *We also allow third parties to place cookies on our websites*, and information collected via these cookies is used to provide you with information that may be of interest to you based on your activities on our websites.**” *Id.* (emphasis added). Quest further explains that the Targeting Cookies “do not directly store personal information . . . but store unique identifiers that identify to us and our partners a particular visitor’s browser and/or device.” *Id.*

Quest’s Privacy Notice states that Quest collects “information online automatically when you visit our websites or applications,” and expressly incorporates the Cookie Notice.¹⁰ Hausmann Decl., Ex. B. Quest explains that it collects information such as “your IP address, browser types, operating system, device types and device IDs or advertising identifiers.” *Id.* The Privacy Notice further explains that Quest collects “**browsing activity . . . what pages you visit and what you click**,” and other “similar information.” *Id.* (emphasis added). Quest then discloses that it uses this data “to provide information, products or services,” “**develop and carry out marketing, advertising and analytics**,” and “deliver content and products or services relevant to your interests.” *Id.* (emphasis added). The Privacy Notice further states that Quest will share information with third parties “to manage or support some of our business operations and services.” *Id.*

2. MyQuest Users Separately Agree to Privacy and Cookie Notices.

Registered MyQuest users separately agree to Quest’s Privacy Notice and Cookie Notice via their agreement to the Account Terms & Conditions. *See* Rigal Decl. ¶¶ 6-8 & Ex B. Specifically, the Account Terms & Conditions contain a section entitled “Use of Your Information/Privacy Policy” which explains:

If You create, transmit, or display information while using the Quest Diagnostics Account Service, You may provide only information that you own or have the right to use. Quest Diagnostics will only use

¹⁰ The version of the Privacy Notice in effect at the time Plaintiffs filed the original Complaint had been in effect since June 8, 2021. Hausmann Decl. ¶¶ 7-8.

information You provide as permitted by the [Online Privacy Policy](#), and applicable law. The purpose of our Online Privacy Policy is to identify the information We collect online, the steps We take to protect it and Your choices regarding how that information is used.

Rigal Decl., Ex. B § 4. The words “Online Privacy Policy” are in blue font and contain a hyperlink that, when clicked, takes the user to Quest’s Privacy Page (questdiagnostics.com/our-company/privacy), which contains links to the Cookie Notice and Privacy Notice, and explains that these notices “provide information about [Quest’s] privacy practices on our websites or applications that link to them.” *Id.* ¶ 9 & Ex. B § 4; Hausmann Decl. ¶¶ 4-5 & Ex. A.

Indeed, there is no dispute that Plaintiffs accepted the Account Terms & Conditions—and the associated Cookie Notice and Privacy Notice—when they created their MyQuest accounts. FAC ¶¶ 4-5. Plaintiffs have never argued otherwise—not even in their opposition to Quest’s motion to transfer venue to this Court or their opposition to Quest’s prior motion to dismiss the FAC. Regardless, Judge Thurston settled that issue when she granted Quest’s motion to transfer, finding “Plaintiffs allege they created MyQuest accounts,” and that “[t]hey do not dispute that they were required to, and did, accept the [Account] Terms and Conditions to create their MyQuest accounts,” including the “relevant privacy policies,” which “were incorporated into Section 4.” *Cole*, 2023 WL 6201702, at *3. The Court found the Account Terms & Conditions are binding because Plaintiffs accepted them. *Id.* at *3, *6.

D. Website Access and the Facebook Pixel

A brief explanation of what happens when a user visits a website is necessary to understand the context of Plaintiffs' claims. Using the example from the FAC, when an individual navigates to a host website such as Quest's General Website, the visitor's internet browser (*e.g.*, Google Chrome, Safari, or Microsoft Edge) "sends a GET request" to the host website "server requesting that [host website] server to load the particular webpage" Uniform Resource Locator ("URL") on the visitor's browser. FAC ¶¶ 15, 17.

The Facebook Pixel is a "piece of code" that website owners such as Quest "can integrate into their website" to help understand certain visitor activity. *Id.* ¶¶ 14-16 & n.16. When visitors access a website that has integrated the Pixel, Facebook's software script directs *the visitor's* "browser to send a separate message to Facebook's servers" containing "the original GET request sent to the host [*i.e.*, Quest's] website" and "additional data that the Pixel is configured to collect." *Id.* ¶ 16. This "additional data" allegedly includes "PageView," "ButtonClick," and "Microdata" information. *Id.* ¶¶ 27-29.

PageView information is the URL (*i.e.*, the specific webpage) accessed by the visitor. *Id.* ¶¶ 24-25. The two examples in the FAC—which, to be clear, are not alleged to be from Plaintiffs' own experiences visiting Quest's websites—are <https://www.questdiagnostics.com/healthcare-professionals/about-our-tests/>

[allergy-asthma](https://myquest.questdiagnostics.com/results/4jkE3XHNNBR97gS1XIO_-Q%3D%3D/prsID/FzMFvgj0FzrJkM4cUzKprQ%3D%3D) and https://myquest.questdiagnostics.com/results/4jkE3XHNNBR97gS1XIO_-Q%3D%3D/prsID/FzMFvgj0FzrJkM4cUzKprQ%3D%3D

Id. ¶ 24, figs. 5 & 6. As to “ButtonClick” and “Microdata” information, Plaintiffs inserted two pictures in the FAC that offer no insight into what additional information they are alleging the Pixel collects beyond the PageView information. *Id.* ¶ 27, figs. 7 & 8. Regardless, Plaintiffs insist that PageView, Microdata, and ButtonClick information is part of “the contents and meaning of a user’s electronic communication.” *Id.* ¶ 29.

E. Plaintiffs’ Experience on Quest’s Websites

Plaintiffs allege that at the time they created their MyQuest accounts they visited Quest’s websites to obtain unspecified diagnostic test results. *Id.* ¶¶ 4-5. Each Plaintiff identically alleges that she “navigated to the General Website”—presumably the homepage—“which redirected her to [MyQuest], where she created an account.” *Id.* Next, each Plaintiff alleges that, after creating an account, she “checked her [diagnostic test] results through [MyQuest].” *Id.* Plaintiffs do not allege additional visits to either the General Website or MyQuest.

Plaintiffs allege that when visitors access MyQuest, the Facebook Pixel “intercept[s] and transmit[s] PageView information” and “transmits the URL accessed.” *Id.* ¶¶ 24-25. Plaintiffs claim that this PageView information “transmits information showing, at a minimum, that a patient has received and is accessing

test results.” *Id.* ¶ 26. Plaintiffs do not allege that the MyQuest information reveals what diagnostic test any visitors took, or what the results were.

As to the General Website, Plaintiffs allege that the Facebook Pixel “intercept[s] and transmit[s] PageView information,” as well as “ButtonClick and Microdata information.” FAC ¶¶ 24, 27. Notably, Plaintiffs do not identify any specific buttons they may have clicked on the General Website such that *their* ButtonClick information might have been intercepted. Plaintiffs do not allege that any PageView information beyond Quest’s homepage, the MyQuest homepage, and the general test results page URL was intercepted. Nor do Plaintiffs identify any Microdata that allegedly was intercepted during *their* visits. Finally, Plaintiffs do not suggest that any information from the General Website revealed what diagnostic test *they* took, or what the results were.

Plaintiffs also allege that the Facebook Pixel “intercept[ed] and collect[ed] personally identifiable information” through the use of first-party and third-party cookies.¹¹ *Id.* ¶¶ 28-30, 38. In support of this allegation, Plaintiffs identify three distinct categories of website visitors. First are visitors who are logged into Facebook when they visit Quest’s websites. These website *visitors* “transmit the c_user cookie”—a third-party cookie—directly “to Facebook, which contains that

¹¹ First-party cookies are created by the website the visitor is visiting (*e.g.*, Quest’s websites). Third-party cookies are “created by a website with a domain name other than the one the visitor is currently visiting” (*e.g.*, Facebook). FAC ¶ 38.

user’s unencrypted Facebook ID,” among other third-party cookies. *Id.* ¶ 31 (emphasis added). The second category consists of visitors who “recently” logged out of their Facebook accounts. For these website visitors, “*Facebook* compels the visitor’s browser to send a smaller set” of third-party cookies *to Facebook*, including the “fr cookie” which contains “an encrypted Facebook ID and browser identifier” and “datar cookies” which “identif[y] a browser.” *Id.* ¶¶ 32-33 (emphases added). The third category consists of website visitors who never created Facebook accounts. For these visitors, the “fr cookie” contains “an abbreviated and encrypted value that identifies the browser,” and the “_fbp cookie” contains “an unencrypted value that uniquely identifies a browser.” *Id.* ¶¶ 34-35. Plaintiffs allege that *Facebook* uses the “c_user”, “fr”, and “_fbp” cookies “to pair event data with personally identifiable information so it can later retarget patients on Facebook.” *Id.* ¶¶ 39-40. Significantly, however, Plaintiffs do not allege that any of the information collected by these cookies was disclosed or used *by Quest*—or even that it was in Quest’s possession in the first place.

F. Plaintiffs’ Facebook Status

Despite Plaintiffs’ distinct descriptions of the different information allegedly shared depending on a website user’s Facebook status (*e.g.*, logged in or logged out), they do not allege whether *they* were logged into Facebook when they visited Quest’s websites. While Plaintiffs now allege that they were Facebook users and

that they “typically” remain logged in “after accessing” their Facebook accounts, FAC ¶¶ 4-5, Plaintiffs do not allege whether they in fact were logged in on the same browser and the same device at the time they accessed Quest’s websites or whether they had recently logged out on the same browser and device (and not cleared their browser cookies), such that any particular type of cookie information (*e.g.*, a Facebook ID as opposed to browser identifier) might have been “intercepted.” This is a material omission because Plaintiffs have not identified what information *about them* allegedly was collected and/or disclosed.

Perhaps more importantly, because Plaintiffs are now alleging that they are Facebook users and access their Facebook accounts, their allegations are sufficient to establish that they consented to certain data being collected by or disclosed to Facebook through the Facebook platform. Indeed, Facebook has an extensive set of contract terms and policies that implicate the collection and sharing of data for registered Facebook users, including a Terms of Service, a Privacy Policy, and a Cookies Policy.¹² For example, the Facebook Terms of Service states that, by using Facebook’s products, “you agree that we can show you ads” and “use your personal data to help determine which personalized ads to show you.” Lattimore Decl., Ex. C. Facebook’s Privacy Policy further explains that the “[t]he

¹² Quest refers to Facebook’s Terms of Service, Privacy Policy, and Cookies Policy in effect at the time Plaintiffs filed the FAC, which are properly subject to judicial notice. *See infra* at pp. 18-19.

information we collect and process about you depends on how you use our Products.” *Id.*, Ex. D. The Privacy Policy states that Facebook collects information about device systems and operations, device identities, and cookie data. *Id.* (“App, browser and device information”). Further, that policy discloses that Facebook “Partners,” such as Quest, may share with Facebook “a variety of your information and activities,” through the use of Facebook’s Business Tools (which include the Pixel) and that “[w]e receive this information whether or not you’re logged in.” *Id.* (“Information from Partners, vendors and third parties.”). Facebook users are informed that those Partners provide “[y]our device information,” “[w]ebsites you visit [(i.e., URL)] and cookie data,” “[p]urchases and transactions you make,” “[t]he ads you see and how you interact with them,” and “[h]ow you use [Facebook’s] Partners’ products and services.” *Id.*

G. Plaintiffs’ Claims

Plaintiffs claim that Quest violated CIPA because it allegedly “aided, agreed with, and conspired with Facebook” to enable Facebook “to track and intercept” internet communication while Plaintiffs and putative class members were accessing Quest’s General Website and MyQuest. FAC ¶ 59. According to Plaintiffs, their communications with Quest’s websites were intercepted “without authorization and consent from Plaintiffs and Class members.” *Id.*

Plaintiffs also claim that Quest violated CMIA, though their allegations here are somewhat confusing. Plaintiffs allege that “Defendant’s Pixel disclosed medical information because it transmitted a patient’s Facebook ID and other Facebook identifiers, which constitutes [*sic*] individually identifiable information, alongside event data that disclosed the URL of the webpage a patient accessed to review test results.” *Id.* ¶ 68. But the only Pixel that Plaintiffs identified in the FAC is the Facebook Pixel, and Facebook is not a defendant here. *See id.* ¶¶ 16-18. Plaintiffs do not allege any facts suggesting that *Quest* ever received or shared with Facebook a patient’s Facebook ID or other Facebook identifiers. And, as noted, Plaintiffs do not allege whether they in fact were logged into their Facebook accounts at the time they accessed Quest’s websites; thus, it is unclear what “identifiers” they are claiming were shared. *Id.* ¶¶ 4-5, 68.

In addition to their individual claims, Plaintiffs seek to represent a putative class of “all persons in California who have navigated and accessed” the General Website and/or MyQuest. *Id.* ¶ 44.

STANDARD OF REVIEW

To survive a motion to dismiss, a plaintiff must assert “more than labels and conclusions” when providing “the grounds of his entitle[ment] to relief.” *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (alteration in original) (internal quotation omitted). “Factual allegations must be enough to raise a right to

relief above the speculative level,” *id.* at 555, and there must be “enough facts” to “nudge [a plaintiff’s] claims across the line from conceivable to plausible.” *Phillips v. Cnty. of Allegheny*, 515 F.3d 224, 234 (3rd Cir. 2008) (quoting *Twombly*, 550 U.S. at 570). Thus, “[w]here a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of entitlement to relief.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal citation and quotation marks omitted). In assessing whether a complaint meets these standards, courts do not accept as true “[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements.” *Rajan v. Crawford*, 2022 WL 16646690, at *3 (3rd Cir. Nov. 3, 2022) (quoting *Iqbal*, 556 U.S. at 678). Indeed, “naked assertions devoid of further factual enhancement” do not suffice. *Iqbal*, 556 U.S. at 678 (internal citation and quotation marks omitted). Moreover, while the Court must accept well-pleaded facts as true, it need not accept legal conclusions. *Mayer v. Belichick*, 605 F.3d 223, 229 (3rd Cir. 2010).

In addition to the allegations of the complaint and documents attached thereto, on a motion to dismiss courts also may consider “undisputedly authentic documents if the complaint’s claims are based upon [them].” *Id.* at 230. Similarly, courts may consider “matters incorporated by reference or integral to the claims, matters of which the Court may take judicial notice, matters of public record,

orders, and other items of record in the case.” *Blue Sky I, LLC v. Jaguar Land Rover N. Am., LLC*, 2016 WL 6803081, at *4 (D.N.J. Nov. 16, 2016); *see also Bambi Baby.com Corp. v. Madonna Ventures, Inc.*, 2019 WL 2337447, at *4 n.5 (D.N.J. June 3, 2019) (“The Court may consider the contents of the Bambi Baby Website because it is ‘integral’ to the Amended Complaint.”).

ARGUMENT

I. Plaintiffs’ Claims Fail Because They Did Not Plausibly Allege Lack of Consent to the Data Collection Practices at Issue.

Plaintiffs have failed to plausibly allege that they did not consent to or authorize the data collection practices associated with their visits to Quest’s websites. In fact, Judge Thurston already found that the Account Terms & Conditions and the associated privacy policies—to which Plaintiffs agreed—“disclose the data collection practices challenged and referenced by Plaintiffs.” *Cole*, 2023 WL 6201702, at *4. This is fatal to both their CIPA and CMIA claims.

By its plain language, CIPA applies only to one “who willfully *and without the consent of all parties* to the communication . . . attempts . . . to learn the contents or meaning of any . . . communication.” Cal Pen. Code § 631(a) (emphasis added). CMIA prohibits a health care provider from disclosing “medical information regarding a patient . . . without first obtaining an authorization,” and further provides that “[e]xcept to the extent expressly authorized by a patient . . . a provider of health care . . . shall not intentionally share, sell, use for marketing, or

otherwise use medical information for a purpose not necessary to provide health care services to the patient.” Cal. Civ. Code § 56.10(a), (d); *see Heller v. Norcal Mut. Ins. Co.*, 8 Cal. 4th 30, 38 (1994) (“to violate [CMIA], a provider of health care must make an unauthorized, unexcused disclosure of privileged medical information”). As California courts have observed, the question of consent is essentially: “Would a reasonable user who viewed [the defendant’s] disclosures have understood that [it] was collecting [the information at issue]?” *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1212 (N.D. Cal. 2014).

To be sure, Plaintiffs say their internet communications with Quest’s websites were intercepted by Facebook “without authorization and consent from Plaintiffs and Class members.” FAC ¶ 59. But this conclusory allegation is little more than a formulaic recitation of the lack of consent elements of a CIPA and CMIA claim. *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 828, 844 (N.D. Cal. 2020) (dismissing CIPA claim and noting that “Plaintiffs’ allegation that the recordings ‘were made without Plaintiffs’ consent’ is conclusory”); *Garcia v. Enter. Holdings, Inc.*, 78 F. Supp. 3d 1125, 1137 (N.D. Cal. 2015) (disclosures in a privacy policy “contradict [the] bare allegation that [plaintiff] did not consent”); *see also Bailey v. CVS Pharmacy, Inc.*, 2018 WL 3866701, at *6-7 (D.N.J. Aug. 14, 2018) (granting motion to dismiss and rejecting conclusory allegation that plaintiff did not consent to receipt of text messages).

The implausibility of Plaintiffs’ conclusory allegations about lack of consent is evident from Quest’s broad disclosures about data collection and the use of third-party cookies to General Website visitors and MyQuest accountholders. For example, Quest’s Cookie Notice states:

We use targeting cookies . . . on our sites to help us promote Quest’s products and services to you on *other sites* and platforms. We also allow third parties to place cookies on our websites, and information collected via these cookies is used to provide you with information that may be of interest to you *based on your activities on our websites*. These targeting cookies . . . store unique identifiers that identify to us and our partners a particular visitor’s browser and/or device.

FAC ¶ 41, fig. 12 (emphasis added). Quest’s Privacy Notice also discloses that Quest collects “information online automatically,” such as “IP address, browser types, operating system, device types and device IDs or advertising identifiers,” and “browsing activity” such as “what pages you visit and what you click.” Hausmann Decl., Ex. B. Quest discloses that it uses this information “to develop and carry out marketing, advertising and analytics” and clearly explains that it may share such information with third parties. *Id.*

Plaintiffs acknowledge the Cookie Notice in the FAC. FAC ¶ 41, figs. 12 & 13. As discussed above, General Website visitors agree to Quest’s Cookie Notice and Privacy Notice when they visit the General Website. Hausmann Decl. ¶¶ 13-14, Exs. G & H. And MyQuest accountholders agree to the Cookie Notice and Privacy Notice during the registration process by agreeing to the Account Terms &

Conditions, *supra* at pp. 4-10. But Plaintiffs inexplicably plead no facts to explain why consent is somehow lacking despite these policies, which disclose the very conduct they challenge—as Judge Thurston already found. *Cole*, 2023 WL 6201702, at *3-4.

In *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954-55, 948-49 (N.D. Cal. 2017), *aff'd* 745 F. Appx. 8 (9th Cir. 2018), the court granted a motion to dismiss CIPA claims arising from Facebook’s collection of the plaintiffs’ web browsing activity on several healthcare websites using Facebook’s Business Tools (such as pixels and cookies). The court found that the plaintiffs’ CIPA and other statutory claims were barred because they consented to Facebook’s activity when they signed up for Facebook accounts and agreed to Facebook’s Cookies Policy and Privacy Policy, which “discloses the precise conduct at issue”—just like Quest’s Cookie Notice and Privacy Notice do here. *Id.* at 953-955. Other California courts interpreting these statutes “consistently hold that terms of service and privacy policies . . . can establish consent to the alleged conduct challenged under various states wiretapping statutes and related claims,” including CIPA. *Silver v. Stripe Inc.*, 2021 WL 3191752, at *4 (N.D. Cal. July 28, 2021) (dismissing federal Wiretap Act and CIPA claim because plaintiffs agreed to a privacy policy that “explicitly state[d] that a consumers’ information may be provided to [the defendant’s] ‘partners’”); *see also Garcia*, 78 F. Supp. 3d at 1136-37 (stating “lack

of consent is an express element of a [CIPA] claim” and finding plaintiff failed to allege lack of consent to sharing of personal data by virtue of the “express provisions” in defendant’s privacy policy); *Perkins*, 53 F. Supp. 3d at 1213-14 (dismissing federal Wiretap Act claim and finding plaintiffs consented to collection of information “[i]n light of the clarity of the disclosure, the proximity of the disclosure to the wrongful conduct, and the ability to opt out”).

Courts in the Third Circuit are in accord, holding that a plaintiff’s consent to data collection depends on the scope of disclosures in a privacy policy. *See Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 118 (W.D. Pa. 2019) (stating general rule that “[a] court must consider the scope of the alleged consent when evaluating a privacy statement.”); *Oliver v. Noom, Inc.*, 2023 WL 8600576, at *9 (W.D. Pa. Aug. 22, 2023) (similar).

Given that Plaintiffs allege they are Facebook users, the holding in *Smith* further weakens their conclusory allegation that they did not consent. Like in *Smith*, Plaintiffs’ claims here are based on *Facebook’s* alleged collection of information. FAC ¶¶ 16-18; *Smith*, 262 F. Supp. 3d at 949. Plaintiffs—as Facebook users and like the plaintiffs in *Smith*—expressly consented to Facebook collecting their browsing activity and other data regarding their website use through tools such as the Pixel. *See Smith*, 262 F. Supp. 3d at 953; *see also* Lattimore Decl., Exs. C to E. Notably, in *Smith* the plaintiffs argued on appeal that

“the collection of health-related data” fell outside of the scope of Facebook’s policies because it was somehow “qualitatively different” or “sensitive.” 745 F. Appx. at 9. The Ninth Circuit rejected that argument, finding that the data could not “reveal details of an individual’s health status or medical history” and, in any event, “many other kinds of information are equally sensitive.” *Id.* In response to the plaintiffs’ claim that such data was subject to the “stringent disclosure requirements” under state and federal statutes pertaining to medical information, the court explained that “the connection between a person’s browsing history and his or her own state of health is too tenuous” to fall within the sweep of health information laws. *See id.* Accordingly, Facebook’s conduct fell “within the scope of Plaintiffs’ consent to Facebook’s Terms and Policies.” *Id.*

Simply put, Plaintiffs did not—and cannot—plausibly allege the requisite lack of consent, nor can they overcome Judge Thurston’s finding that “the [Account] Terms and Conditions disclose the data collection practices challenged and referenced by Plaintiffs.” *Cole*, 2023 WL 6201702, at *4. Accordingly, the Court should dismiss Plaintiffs’ CIPA and CMIA claims.

II. Plaintiffs’ CIPA Claim Fails Because Under Third Circuit Law Facebook Was A Party to the Communications At Issue.

Plaintiffs’ theory is that Quest violated CIPA by “aiding and assisting *Facebook’s* eavesdropping” of their website communications with Quest simply by installing the Pixel. FAC ¶¶ 29, 59-60 (emphasis added). The Third Circuit

previously addressed an internet tracking cookies dispute involving essentially the same technology and held that no “eavesdropping” occurred in violation of CIPA (and the federal Wiretap Act) because the party in Facebook’s position was the “intended recipient” of—and thus a party to—the communication at issue. *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 152 (3d Cir. 2015). Under *Google Cookie*, Plaintiffs’ CIPA claim fails as a matter of law.

Plaintiffs claim that *Facebook* is the eavesdropper here and allege that Facebook was able to “intercept” Plaintiffs’ website communications with Quest because Quest installed the Pixel on its websites. FAC ¶¶ 29-30. But critically, Plaintiffs’ allegations make clear that the technological communications they take issue with are “a separate message” between Plaintiffs *and Facebook*, not Plaintiffs and Quest. *Id.* ¶ 16. Indeed, Plaintiffs complain that the Pixel and its associated cookies cause *Plaintiffs’* internet browsers, to send a “***second***, secret transmission” directly *to Facebook* “contain[ing] the original GET request sent to [Quest].” FAC ¶¶ 16-17 (emphasis added).

In *Google Cookie*, the plaintiffs sued Google and other internet advertisers for violating the federal Wiretap Act and CIPA, alleging that they used similar “third-party web tracking” that enabled them “to record information that [plaintiffs] exchanged with first-party websites . . . which defendants intercepted while not a party to those communications.” *Id.* at 140. Similar to here, the

plaintiffs alleged that “the server hosting the publisher’s webpage . . . instruct[ed] the user’s web browser to send a GET request to Google” via the placement of “cookies on web browsers.” *Id.*; see FAC ¶¶ 16-17. The Third Circuit engaged in a detailed and careful analysis of the technology and the various communications at issue, finding that:

If user’s browsers *directly communicate* with the defendants about the webpages they are visiting—as the complaint pleads with particularity—then there is no need for the defendants to acquire that information from transmissions to which they are not a party. . . . Here, the operative allegations of the complaint support only the conclusion that the defendants acquired the plaintiffs’ internet history information by way of GET request that the *plaintiffs sent directly to the defendants.*”

Google Cookie, 806 F.3d at 140-42 (emphases added). The Court held that because Google and the other defendants “were the intended recipients of the GET requests they acquired” through the use of cookies and “were parties to any communications that they acquired” there was no unlawful interception or eavesdropping, and thus no violation of the Wiretap Act or CIPA. *Id.* at 143, 145, 152.

Applying *Google Cookie* here, Facebook did not engage in an unlawful “interception” or “eavesdropping” because Facebook was an intended recipient of the communications at issue, which Plaintiffs’ browser sent *directly to Facebook* as a “separate message.” FAC ¶¶ 16-17. Since Facebook did not engage in an unlawful “interception” or “eavesdropping” in violation of CIPA, it necessarily

follows that Quest could not have violated CIPA for purportedly “aiding and assisting Facebook’s eavesdropping.” *See id.* ¶ 60. Accordingly, Plaintiffs’ CIPA claim fails as a matter of law and must be dismissed under *Google Cookie*.

III. Plaintiffs’ CIPA Claim Fails Because They Did Not Plausibly Allege that the “Contents” of Their Communications Were Intercepted.

CIPA is implicated only if the alleged violator “learn[s] the *contents* or meaning of any message, report, or communication.” Cal. Pen. Code § 631(a) (emphasis added). Plaintiffs’ CIPA claim fails because they did not—and cannot—plausibly allege that Facebook learned the “contents” of any of Plaintiffs’ communications with Quest’s websites.

The Ninth Circuit has found that “contents” means “the intended message conveyed by the communication” as opposed to “record information regarding the characteristics of the message that is generated in the course of the communication.” *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014).¹³ In the context of website communications, “[c]ourts employ a contextual ‘case-specific’ analysis hinging on ‘how much information would be revealed’ by the information’s tracking and disclosure” to determine whether it constitutes the

¹³ Although *Zynga* interpreted the definition of “contents” in the federal Wiretap Act, courts recognize that “CIPA’s wiretapping provision and the federal Wiretap Act [both] preclude identical conduct.” *E.g., In re Nickelodeon Consumer Privacy Litig.*, 2014 WL 3012873, at *17 (D.N.J. July 2, 2014), *aff’d* 827 F.3d 262 (3d Cir. 2016); *Brodsky v. Apple, Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020).

“contents” of a communication. *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1092 (N.D. Cal. 2022).

For example, in *Zynga*, the Ninth Circuit held that “the address of the webpage” (*i.e.*, the URL) did “not meet the definition of ‘contents,’ because these pieces of information are not the ‘substance, purport, or meaning’ of a communication.” *Id.* at 1107. The court recognized that a referer header (which includes the URL) could disclose that a person viewed the “page of a gay support group,” but nevertheless concluded that such URLs “function[] like an ‘address,’” and not “content.” *Id.* at 1107-08. The *Zynga* court acknowledged there could be circumstances where a URL potentially “could amount to a disclosure of the contents of a communication” if, for example it divulged specific search terms input by the visitor. *Id.* at 1108-09.

The Third Circuit, relying in part on *Zynga*, has held that “some *queried* URLs qualify as content” if they “involve reproduction of a search phrase entered by a user into a search engine.” *Google Cookie*, 806 F.3d at 137-39 (emphasis added). In *In re Nickelodeon Consumer Privacy Litigation*, 2014 WL 3012873, at *14-15, *17 (D.N.J. July 2, 2014), *aff’d* 827 F.3d 262 (3d Cir. 2016), the court dismissed federal Wiretap Act and CIPA claims because there were “no allegations that Defendants intercepted ‘contents’ of communications.” In so holding, the court relied on *Zynga* for the proposition that, while a URL containing particular

search terms could constitute “contents,” the static file path and video title information at issue did not meet that bar. *Id.* at *15. *See also Hammerling*, 615 F. Supp. 3d at 1093 (dismissing CIPA claim because even though defendant “might infer a user’s traits and habits” from the data collected, plaintiffs did not allege that it “can read the specific information (*i.e.*, content) that a user inputs” and thus failed to plead that it learned the “‘content’ of a communication”).

Similar to *Zynga*, *Hammerling*, and *Nickelodeon*, Plaintiffs here do not plausibly allege that Facebook learned the “contents” of their website communications. Their allegation that Facebook intercepts a “GET request” and PageView information which “transmits the URL accessed,” FAC ¶¶ 16, 24- 25, is no different than the URL information the Ninth Circuit held did not amount to a disclosure of “contents” in *Zynga*, 750 F. 3d at 1108-09. Indeed, Plaintiffs have not alleged that the URLs at issue were queried URLs containing search terms entered by users into a search engine or contained any other user-generated inputs, as opposed to merely containing the address of a page a user visited. Thus, their CIPA claim fails consistent with *Zynga*, *Hammerling*, and *Nickelodeon*. *See also Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082 (C.D. Cal. 2021) (CIPA “protects only the internal, *user-generated* material of a message, not routine identifiers, whether automatically generated or not.” (emphasis added)).

As to “ButtonClick” and “Microdata” information, Plaintiffs’ allegations similarly do not establish that any “content” was collected. FAC ¶ 27. Beyond the PageView information, which is insufficient, they allege only that “the title of the page, keywords *associated with the page*, and a description *of the page*” was shared with Facebook. FAC ¶ 28 (emphases added). But these are not *Plaintiffs’* communication contents or user-generated material; they are merely further information about the page visited. *See Yoon*, 549 F. Supp. 3d at 1077, 1082-83 (holding that “keystrokes and clicks; pages viewed; shipping and billing information; date, time, and duration of visit; IP address and physical location; and browser type and operating system” are not message “content” under CIPA).

As to Plaintiffs’ allegations concerning what certain cookies allegedly collect for the three distinct categories of website users, FAC ¶¶ 30-35, Plaintiffs do not allege that any of the information collected by these cookies—such as a user’s Facebook ID or a browser identifier—was part of any communication between Plaintiffs and Quest (as opposed to a communication between Plaintiffs and Facebook, which Facebook could not “intercept” as a matter of law under *Google Cookie*). Additionally, due to Plaintiffs’ failure to allege whether they were logged into Facebook or recently logged out during interactions with Quest’s websites, it is not even clear what “content” of their communications Plaintiffs are alleging was intercepted. *See Smith v. Trusted Universal Standards in Elec.*

Transactions, Inc., 2010 WL 1799456, at *11 (D.N.J. May 4, 2010) (dismissing a Wiretap Act claim where plaintiff asserted “in a conclusory fashion” that defendant monitored his internet communications).

IV. Plaintiffs’ CMIA Claim Fails Because None of the Information Allegedly Disclosed or Used Constitutes “Medical Information.”

CMIA defines “medical information” as “individually identifiable information . . . in possession of or derived from a provider of health care . . . regarding a patient’s medical history, . . . mental or physical condition, or treatment.” Cal. Civ. Code § 56.05(j). “Individually identifiable,” in turn, “means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual.” *Id.* The information Plaintiffs allege that Facebook intercepted does not qualify as “medical information” under CMIA because it does not reveal any substantive information regarding a website visitor’s medical history, condition, or treatment. *See id.* Moreover, Plaintiffs do not allege that any of *their* individually identifiable information was disclosed or used.

In *Eisenhower Medical Center v. Superior Court*, a California Court of Appeal agreed that “medical information” under CMIA “is *substantive information* regarding a patient’s medical condition or history that is *combined with* individually identifiable information.” 226 Cal. App. 4th 430, 434 (Cal. Ct. App., 4th Dist. 2014) (emphases added). In *Eisenhower*, patient data was stolen from a

medical center, including names, medical record numbers, birthdates, and last four digits of Social Security Numbers. *Id.* at 432. Although the information disclosed was individually identifiable, the court held that it was not “medical information” because it “does not reveal medical history, diagnosis, or care.” *Id.* at 435.

Critically, the court found that “[c]onfirmation that a person’s medical record exists somewhere is not medical information as defined under the CMIA,” nor is “the mere fact that a person may have been a patient.” *Id.* Similarly, in *Wilson v. Rater8, LLC*, 2021 WL 4865930, at *1, *5 (S.D. Cal. Oct. 18, 2021), the court found that “treating physician names, medical treatment appointment information, and medical treatment discharge dates and times” did not constitute “medical information” under CMIA even though some of it was individually identifiable. Compare *Kurowski v. Rush Sys. for Health*, -- F. Supp. 3d --, 2023 WL 4707184, at *1, *3 (N.D. Ill. July 24, 2023) (finding that “IP addresses, patient cookie identifiers, device identifiers, account numbers, URLs” transmitted to Facebook and other third parties through online tracking tools were not “individually identifiable health information” under HIPAA) and *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2023 WL 8540911, at *8 (D.N.J. May 5, 2023) (alleged disclosure of personal information, including diagnostic “codes from which the specific medical diagnosis could be identified,” was sufficient to allege disclosure of “medical information” under CMIA).

As in *Eisenhower* and *Wilson*, Plaintiffs here do not identify any disclosure of “substantive information” regarding their medical history, condition, or treatment. Plaintiffs allege that when visitors access MyQuest, the Pixel “intercept[s] and transmit[s] PageView information” and “transmits the URL accessed.” FAC ¶¶ 24-25.¹⁴ But Plaintiffs do not allege that any *substantive* information—such as what test a visitor took or what the results were—was disclosed in the URL itself or otherwise. Even assuming “the URL of the webpage a patient accessed to review test results” was disclosed, *id.* ¶ 68, it is not materially different than the information disclosed in *Eisenhower*, which revealed that the person was a patient and that a “medical record exists somewhere.” *Eisenhower*, 226 Cal. App. 4th at 436. And it is far less revealing than the detailed information disclosed in *Wilson*, which the court held was not medical information under CMIA. *Wilson*, 2021 WL 4865930, at *5. *See also Smith*, 262 F. Supp. 3d at 955 (“Nothing about the URLs, or the content of the pages located at those URLs,

¹⁴ Plaintiffs’ CMIA claim relates to accessing MyQuest in that they complain about disclosure of “the URL of the webpage a patient accessed to review test results.” FAC ¶ 68. The only potentially relevant URL identified in the FAC is in Figure 6, which contains the words “myquest.questdiagnostics.com/results/” followed by an indecipherable string of letters, numbers, and symbols. The word “results” plainly is not “medical information” and Plaintiffs do not claim that the string of letters, numbers, and symbols reveals medical information either. The other URL in Figure 5 is a URL from the General Website that is not alleged to reveal “medical information” within the meaning of CMIA.

relates ‘to the past, present, or future physical or mental health or condition of an individual.’”) (emphasis in original, footnote and citation omitted).

Additionally, Plaintiffs do not plausibly allege facts indicating that any of *their* individually identifiable information was actually disclosed, which is fatal to their claims. *Cf. Bycko v. State Farm Mut. Auto. Ins. Co.*, 2023 WL 7411752, at *6 (D.N.J. Nov. 9, 2023) (dismissing privacy claims for lack of standing because plaintiffs “fail[ed] to allege that *their* information was in fact disclosed” and did “not specify what information, confidential or otherwise, which may have been disseminated” (emphasis added)). Plaintiffs’ theory is that “a patient’s Facebook ID and other Facebook identifiers” are personal identifying information that is shared as result of certain cookies, such as the “c_user,” “fr” and “_fbp” cookies. FAC ¶¶ 30-40, 68. However, Plaintiffs do not allege that *they*, in fact, were logged in to Facebook at or near the time they visited Quest’s websites, thus they have not plausibly alleged that *their* unencrypted Facebook ID was shared by the “c_user” cookie. *See id.* ¶ 31. Moreover, Plaintiffs have not plausibly alleged that any encrypted or unencrypted Facebook ID was shared because they did not allege facts regarding the timing of their website visits in relation to their Facebook login status, whether they visited Quest’s websites using the same browser or device they used to visit Facebook, or whether they cleared cookies. *See id.* ¶¶ 4-5. In this regard, if for example Plaintiffs visited Quest’s websites on a different browser

than they used to login to Facebook or after having cleared cookies, only a browser identifier would have been shared. *Id.* ¶ 35. But it is well settled that browser identifiers alone are not sufficient to identify a person. *Nickelodeon*, 827 F.3d at 285 (“static digital identifiers” are not “personally identifiable information”); *In re Hulu Privacy Litig.*, 2014 WL 1724344, at *11 (N.D. Cal. Apr. 28, 2014) (“a unique anonymized ID alone is not [personally identifiable information]”); *Eichenberger v. ESPN, Inc.*, 2015 WL 7252985, at *5 (W.D. Wash. May 7, 2015) (“device serial number” is not personally identifiable information).

Finally, Plaintiffs allege that Quest removed the Pixel from MyQuest “sometime after December 2021,” and Plaintiff Roche’s visit to MyQuest allegedly occurred in March 2022. FAC ¶¶ 5, 23 n.21; *see supra* at p. 4 n.5. These allegations suggest Plaintiff Roche’s personal identifying information may not have been shared at all. Regardless, absent plausible allegations that Roche’s personal identifying information was, in fact, shared, her CMIA claim fails as a matter of law and should be dismissed.

V. Plaintiffs’ CMIA Claim Fails Because They Do Not Allege that Quest Was the Party that Disclosed or Used the Information At Issue.

Again, Plaintiffs are claiming that *Facebook* intercepted the information at issue, and that Quest aided and abetted Facebook by installing the Pixel on Quest’s websites. FAC ¶¶ 16-17, 68. Although CIPA’s specific language has led the Ninth Circuit to conclude that it creates an aiding and abetting claim, CMIA does not

contain similar language. By its plain terms, CMIA only prohibits a *health care provider* from improperly disclosing or using medical information. Cal. Civ. Code § 56.10(a) (“A provider of health care . . . shall not disclose”); Cal. Civ. Code § 56.10(d) (provider of health care shall not “share” or “sell” medical information or “use [it] for marketing”). “Disclose” means “an affirmative act of communication.” *Regents of Univ. of Cal. v. Superior Court*, 220 Cal. App. 4th 549, 564 (Cal. Ct. App., 2d Dist. 2013). Indeed, to state a CMIA claim “the plaintiff must plead an ‘affirmative communicative act’ *by the defendant*.” *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 922 (S.D. Cal. 2020) (emphasis added).

In support of their CMIA claim, Plaintiffs allege that “Defendant’s Pixel disclosed medical information,” FAC ¶ 68, but the Court need not accept this conclusory allegation, especially since it is inconsistent with Plaintiffs’ other allegations. Indeed, the only Pixel that Plaintiffs identify belongs to Facebook, not Quest. *Id.* ¶¶ 16-17. Moreover, as noted above, Plaintiffs’ theory is that “a patient’s Facebook ID and other Facebook identifiers” are personal identifying information. *Id.* ¶ 68. But Plaintiffs do not allege any facts suggesting that Quest ever disclosed or used (much less received) a patient’s Facebook ID or other Facebook identifiers. Indeed, Plaintiffs’ allegations make clear that the communications at issue are actually between Plaintiffs *and Facebook*, not Plaintiffs and Quest. FAC ¶¶ 16-17.

Accordingly, Quest cannot be said to have “disclosed” any information. *See* Cal. Civ. Code § 56.10(a); *Google Cookie*, 806 F.3d at 140-2 (“the defendants acquired the plaintiffs’ [information] when . . . the plaintiffs’ browsers sent that information directly to the defendants’ servers”). Because Plaintiffs plainly are not challenging any improper disclosure or use by Quest, their CMIA claim fails as a matter of law.

VI. Plaintiffs’ California Claims Fail Because New Jersey Law Applies.

The MyQuest Account Terms & Conditions state: “This Agreement and the resolution of any and all disputes related to this Agreement shall be construed in accordance with the laws of the State of New Jersey” and “You agree that the statutes and laws of the State of New Jersey, without regard to any principles of conflicts of law, will apply to any and all matters relating to the use of the Account Service.” Rigal Decl., Ex. B § 12. The terms and conditions on the General Website similarly state that New Jersey law “will apply to all matters relating to the use of this site.” *See supra* at p. 6 n.7. Under New Jersey law,¹⁵ this Court should enforce this contractual choice of law. *Collins v. Mary Kay, Inc.*, 874 F.3d 176, 183-84 (3d Cir. 2017) (explaining that “[o]rdinarily, when parties to a contract have agreed to be governed by the laws of a particular state, New Jersey courts will

¹⁵ A district court sitting in diversity “look[s] to the choice-of-law rules of the forum state—the state in which the District Court sits—in order to decide which body of substantive law to apply to a contract provision.” *Collins*, 874 F.3d at 183.

uphold the contractual choice.”). Because New Jersey law governs this dispute, Plaintiffs’ California statutory claims fail.

New Jersey courts will enforce a choice-of-law clause unless one of the exceptions found in Restatement (Second) Conflicts § 187(2) applies. *Homa v. Am. Express Co.*, 558 F.3d 225, 227 (3d Cir. 2009), *abrogated on other grounds by AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011) (similar language). Under Section 187(2), the contractual choice may not be overridden unless:

(a) the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties’ choice, or

(b) application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue and which . . . would be the state of the applicable law in the absence of an effective choice of law by the parties.

2 RST Conflicts § 187(2). Plaintiffs have the burden to show that one of the Section 187(2) exceptions applies. *Collins*, 874 F.3d at 184 (upholding contractual choice-of-law clause where plaintiff “ha[d] not demonstrated that either of the two exceptions outlined in Restatement § 187(2) should apply”).

Quest is headquartered in New Jersey. This is dispositive of the Section 187(2)(a) inquiry, establishing that New Jersey has a “substantial relationship” to the dispute. *Diversant, LLC v. Carino*, 2018 WL 1610957, at *3 (D.N.J. Apr. 2, 2018) (“The exception in part (a) does not apply here because Plaintiff is a New

Jersey limited liability company headquartered in New Jersey, and therefore New Jersey has a ‘substantial relationship’ to the parties.”).

To establish the Section 187(2)(b) exception, the party seeking application of a different state’s law from the choice made in a contract must show “(1) that California has a materially greater interest than New Jersey in the determination of this dispute, (2) that application of New Jersey law on the [issue at hand] would be contrary to California’s public policy, and (3) that California law would apply in the absence of an effective choice of law clause.” *Diversant*, 2018 WL 1610957, at *3. Plaintiffs cannot establish any of these elements here.

It is true of course that Plaintiffs reside in California, FAC ¶¶ 4-5, but that is insufficient to demonstrate that California has a “materially greater” interest in the dispute than New Jersey, where Quest is headquartered. *See Coface Collections N. Am. Inc. v. Newton*, 430 F. App’x 162, 168 (3d Cir. 2011) (holding that Louisiana did not have a “materially greater interest” where plaintiff was “a national company” and “Delaware has a substantial interest in enforcing this voluntarily negotiated contract clause that explicitly designates Delaware law to govern”). Plaintiffs likewise cannot show that application of New Jersey law to their use of Quest’s website would be contrary to California public policy, or that California law would apply in the absence of a choice of law clause. For example, New Jersey has its own wiretapping law. *See* N.J.S.A. 2A:156A-3. The mere fact that the

chosen law might provide “greater or lesser protection than California law, or that in a particular application the chosen law would not provide protection while California law would, are not reasons for applying California law.” *Medimatch, Inc. v. Lucent Techs. Inc.*, 120 F. Supp. 2d 842, 862 (N.D. Cal. 2000) (finding that application of New Jersey consumer protection law would not violate California’s public policy towards consumers).

Because Plaintiffs cannot overcome their agreement to be governed by New Jersey law with regard to their use of Quest’s websites, their California statutory claims necessarily fail as a matter of law. As a result, the Court should dismiss the FAC in its entirety.

CONCLUSION

For the foregoing reasons, Defendant Quest Diagnostics Incorporated respectfully requests that the Court dismiss the FAC in its entirety.

Dated: February 5, 2024

FAEGRE DRINKER BIDDLE & REATH LLP

By: /s/ Matthew J. Fedor
Matthew J. Fedor
Zoë K. Wilhelm

*Attorneys for Defendant
Quest Diagnostics Incorporated*